Distribution of Modular Inverses and Multiples of Small Integers and the Sato–Tate Conjecture on Average

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

February 8, 2008

Abstract

We show that, for sufficiently large integers m and X, for almost all $a = 1, \ldots, m$ the ratios a/x and the products ax, where $|x| \leqslant X$, are very uniformly distributed in the residue ring modulo m. This extends some recent results of Garaev and Karatsuba. We apply this result to show that on average over r and s, ranging over relatively short intervals, the distribution of Kloosterman sums

$$K_{r,s}(p) = \sum_{n=1}^{p-1} \exp(2\pi i(rn + sn^{-1})/p),$$

for primes $p \leqslant T$ is in accordance with the Sato–Tate conjecture.

1 Introduction

1.1 Motivation

A rather old conjecture asserts that if $m = p$ is prime then for any fixed $\varepsilon > 0$ and sufficiently large p, for every integer a there are integers x and y with $|x|, |y| \leqslant p^{1/2+\varepsilon}$ and such that $a \equiv xy \pmod p$, see [13, 15, 16, 17]

and references therein. The question has probably been motivated by the following observation. Using the Dirichlet pigeon-hole principle, one can easily show that for every integer a there are integers x and y with $|x|, |y| \leqslant 2p^{1/2}$ with $a \equiv y/x \pmod p$.

Unfortunately, this is known only with $|x|, |y| \geqslant Cp^{3/4}$ for some absolute constant $C > 0$, which is due to Garaev [14].

On the other hand, it has been shown in the series of works [13, 15, 16, 17] that the congruence $a \equiv xy \pmod p$ is solvable for all but $o(m)$ values of $a = 1, \ldots, m-1$, with x and y significantly smaller than $m^{3/4}$. In particular, it is shown by Garaev and Karatsuba [16] for x and y in the range $1 \leqslant x, y \leqslant m^{1/2}(\log m)^{1+\varepsilon}$. Certainly this result is very sharp. Indeed, it has been noticed by Garaev [13] that well known estimates for integers with a divisor in a given interval immediately imply that for any $\varepsilon > 0$ almost all residue classes modulo m are not of the form $xy \pmod m$ with $1 \leqslant x, y \leqslant m^{1/2}(\log m)^{\kappa-\varepsilon}$ where

$$\kappa = 1 - \frac{1 + \log\log 2}{\log 2} = 0.08607\ldots.$$

One can also derive from [9] that for any $\varepsilon > 0$ the inequality

$$\max\{|x|, |y| \ : \ xy \equiv 1 \pmod m\} \geqslant m^{1/2}(\log m)^{\kappa/2}(\log\log m)^{3/4-\varepsilon}$$

holds:

- for all positive integers $m \leqslant M$, except for possibly $o(M)$ of them,
- for all prime $m = p \leqslant M$ except for possibly $o(M/\log M)$ of them.

Similar questions about the ratios x/y, have also been studied, see [13, 16, 27].

1.2 Our results

It is clear that these problems are special cases of more general questions about the distribution in small intervals of residues modulo m of ratios a/x and products ax, where $|x| \leqslant X$. In fact here we consider this more x from more general sets $\mathcal{X} \subseteq [-X, X]$.

Accordingly, for integers a, m, Y and Z and a set of integers $\mathcal{X}$, we denote

$$\begin{aligned} M_{a,m}(\mathcal{X};Y,Z) &= \#\{x \in \mathcal{X} \ : \ a/x \equiv y \pmod m, \\ &\qquad\qquad \gcd(x,m)=1,\ y \in [Z+1, Z+Y]\}, \\ N_{a,m}(\mathcal{X};Y,Z) &= \#\{x \in \mathcal{X} \ : \ ax \equiv y \pmod m, \\ &\qquad\qquad y \in [Z+1, Z+Y]\} \end{aligned}$$

where the inversion is always taken modulo m.

We note that although in general the behaviour of $N_{a,m}(\mathcal{X};Y,Z)$ is similar to the behaviour of $M_{a,m}(\mathcal{X};Y,Z)$, there are some substantial differences. For example, if $\mathcal{X} = \{x \in \mathbb{Z} \ : \ |x| \leqslant X\}$ for some $X \geqslant 1$, then $N_{a,m}(\mathcal{X};X,0) = 0$ for all integer a with $m - m/X - 1 < a \leqslant m-1$, see the argument in [13, Section 4]. It is also interesting to remark that the question of asymptotic behaviour of $N_{a,m}(\mathcal{X};Y,Z)$ has some applications to the discrete logarithm problem, see [28].

Here we extend some of the results of Garaev and Karatsuba [16] and show that if $X, Y \geqslant m^{1/2+\varepsilon}$ and $\mathcal{X}$ is a sufficiently massive subset of the interval $[-X, X]$, then $M_{a,m}(\mathcal{X};Y,Z)$ and $N_{a,m}(\mathcal{X};Y,Z)$ are close to their expected average values for all but $o(m)$ values of $a = 1, \ldots, m$.

It seems that the method of Garaev and Karatsuba [16] is not suitable for obtaining results of this kind. So we use a different approach which is somewhat similar to that used in the proof of [4, Theorem 1].

Finally we note that one can also obtain analogous results for

$$\begin{aligned} N^*_{a,m}(\mathcal{X};Y,Z) &= \#\{x \in \mathcal{X} \ : \ ax \equiv y \pmod m, \\ &\qquad\qquad \gcd(x,m)=1,\ y \in [Z+1, Z+Y]\} \end{aligned}$$

and several other similar quantities.

1.3 Applications

For integers r and s and a prime p, we consider Kloosterman sums

$$K_{r,s}(p) = \sum_{n=1}^{p-1} \mathbf{e}_p(rn + sn^{-1})$$

where as before the inversion is taken modulo p. We note that for the complex conjugated sum we have

$$\overline{K_{r,s}(p)} = K_{-r,-s}(p) = K_{r,s}(p)$$

thus $K_{r,s}(p)$ is real.

Since accordingly to the Weil bound, see [19, 22, 23, 25], we have

$$|K_{r,s}(p)| \leqslant 2\sqrt{p}, \qquad \gcd(r,s,p)=1,$$

we can now define the angles $\psi_{r,s}(p)$ by the relations

$$K_{r,s}(p) = 2\sqrt{p}\cos\psi_{r,s}(p) \qquad \text{and} \qquad 0 \leqslant \psi_{r,s}(p) \leqslant \pi.$$

The famous *Sato–Tate* conjecture asserts that, for any fixed non-zero integers r and s, the angles $\psi_{r,s}(p)$ are distributed accordingly to the *Sato–Tate density*

$$\mu_{ST}(\alpha,\beta) = \frac{2}{\pi}\int_\alpha^\beta \sin^2\gamma\, d\gamma,$$

see [19, Section 21.2]. That is, if $\pi_{r,s}(\alpha,\beta;T)$ denotes the number of primes $p \leqslant T$ with $\alpha \leqslant \psi_{r,s}(p) \leqslant \beta$, where, as usual $\pi(T)$ denotes the total number of primes $p \leqslant T$, the Sato–Tate conjecture predicts that

$$\pi_{r,s}(\alpha,\beta;T) \sim \mu_{ST}(\alpha,\beta)\pi(T), \qquad T \to \infty, \tag{1}$$

for all fixed real $0 \leqslant \alpha < \beta \leqslant \pi$, see [19, Section 21.2]. It is also known that if p is sufficiently large and r and s run independently through $\mathbb{F}_p^*$ then the distribution of $\psi_{r,s}(p)$ is accordance with the Sato–Tate conjecture, see [19, Theorem 21.7]. An explicit quantitative bound on the discrepancy between the distribution of $\psi_{r,s}(p)$, $r,s \in \mathbb{F}_p^*$ and the Sato–Tate distribution is given by Niederreiter [26]. Various modifications and generalisations of this conjecture are given by Katz and Sarnak [22, 23]. Despite a series of significant efforts towards this conjecture, it remains open, for example, see [2, 6, 10, 11, 22, 23, 24, 26] and references therein.

Here, combining our bounds of $M_{a,m}(\mathcal{X};Y,Z)$ with a result of Niederreiter [26], we show that on average over r and s, ranging over relatively short intervals $|r| \leqslant R$, $|s| \leqslant S$, the Sato-Tate conjecture holds on average and the sum

$$\Pi_{\alpha,\beta}(R,S,T) = \frac{1}{4RS}\sum_{0<|r|\leqslant R}\sum_{0<|s|\leqslant S}\pi_{r,s}(\alpha,\beta;T)$$

satisfies

$$\Pi_{\alpha,\beta}(R,S,T) \sim \mu_{ST}(\alpha,\beta)\pi(T).$$

Furthermore, over a larger intervals, we also estimate the dispersion

$$\Delta_{\alpha,\beta}(R,S,T) = \frac{1}{4RS} \sum_{0<|r|\leqslant R} \sum_{0<|s|\leqslant S} \left(\pi_{r,s}(\alpha,\beta;T) - \mu_{ST}(\alpha,\beta)\pi(T)\right)^2 .$$

We recall that Fouvry and Murty [12] have the *Lang–Trotter conjecture* on average over $|r| \leqslant R$ and $|s| \leqslant S$ for the family of elliptic curves $\mathbb{E}_{r,s}$ given by the *affine Weierstraß equation*:

$$\mathbb{E}_{r,s} \ : \ U^2 = V^3 + rV + s.$$

Several more interesting questions on elliptic curves have been studied "on average" for similar families of curves in [1, 3, 5, 7, 8, 18, 20, 21].

However, we note that technical details of our approach are different from that of Fouvry and Murty [12]. For example, their result is nontrivial only if

$$RS \geqslant T^{3/2+\varepsilon} \qquad \text{and} \qquad \min\{R,S\} \geqslant T^{1/2+\varepsilon}$$

for some fixed $\varepsilon > 0$. The technique of [12] can also be applied to getting an asymptotic formula for $\Pi_{\alpha,\beta}(R,S,T)$ for the same range of parameters R, S and T. Apparently it can also be applied to $\Delta_{\alpha,\beta}(R,S,T)$ but certainly in an even narrower range of parameters. On the other hand, our results for $\Pi_{\alpha,\beta}(R,S,T)$ and $\Delta_{\alpha,\beta}(R,S,T)$ are nontrivial for

$$RS \geqslant T^{1+\varepsilon} \tag{2}$$

and

$$RS \geqslant T^{2+\varepsilon} \tag{3}$$

respectively.

1.4 Notation

Throughout the paper, any implied constants in symbols O and $\ll$ may occasionally depend, where obvious, on the real positive parameter ε and are absolute otherwise. We recall that the notations $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \leqslant cV$ holds with some constant $c > 0$.

We use p, with or without a subscript, to denote a prime number and use m to denote a positive integer.

Finally, as usual, $\varphi(m)$ denotes the Euler function of m.

1.5 Acknowledgements

The author wishes to thank Moubariz Garaev for many useful discussions.

This work was supported in part by ARC grant DP0556431.

2 Congruences

2.1 Inverses

We start with the estimate of the average deviation between $M_{a,m}(\mathcal{X}; Y, Z)$ and its expected value taken over $a = 1 \ldots, m$. If the set $\mathcal{X} \subseteq [-X, X]$ is dense enough, for example, if $\#\mathcal{X} \geqslant X m^{o(1)}$, this bound is nontrivial for $X, Y \geqslant m^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large m.

Theorem 1. *For all positive integers m, X, Y, an arbitrary integer Z and a set $\mathcal{X} \subseteq \{x \in \mathbb{Z} \ : \ |x| \leqslant X\}$,*

$$\sum_{a=1}^{m} \left| M_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}_m \frac{Y}{m} \right|^2 \leqslant \#\mathcal{X}(X + Y) m^{o(1)}.$$

where

$$\mathcal{X}_m = \{x \in \mathcal{X} \ : \ \gcd(x, m) = 1\}.$$

Proof. We denote

$$\mathbf{e}_m(z) = \exp(2\pi i z/m).$$

Using the identity

$$\frac{1}{m} \sum_{-(m-1)/2 \leqslant h \leqslant m/2} \mathbf{e}_m(hv) = \begin{cases} 1 & \text{if } v \equiv 0 \pmod m, \\ 0 & \text{if } v \not\equiv 0 \pmod m, \end{cases}$$

we write

$$\begin{aligned} M_{a,m}(\mathcal{X}; Y, Z) &= \sum_{x \in \mathcal{X}_m} \sum_{y=Z+1}^{Z+Y} \frac{1}{m} \sum_{-(m-1)/2 \leqslant h \leqslant m/2} \mathbf{e}_m\left(h(ax^{-1} - y)\right) \\ &= \frac{1}{m} \sum_{-(m-1)/2 \leqslant h \leqslant m/2} \sum_{x \in \mathcal{X}_m} \mathbf{e}_m\left(hax^{-1}\right) \sum_{y=Z+1}^{Z+Y} \mathbf{e}_m(-hy) \\ &= \frac{1}{m} \sum_{-(m-1)/2 \leqslant h \leqslant m/2} \mathbf{e}_m(-hZ) \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^{X} \mathbf{e}_m\left(hax^{-1}\right) \sum_{y=1}^{Y} \mathbf{e}_m(-hy). \end{aligned}$$

The term corresponding to $h = 0$ is

$$\frac{1}{m} \sum_{x \in \mathcal{X}_m} \sum_{y=1}^{Y} 1 = \#\mathcal{X}_m \frac{Y}{m}.$$

Hence

$$M_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}_m \frac{Y}{m} \ll \frac{1}{m} E_{a,m}(X, Y),$$

where

$$E_{a,m}(X, Y) = \sum_{1 < |h| \leqslant m/2} \left| \sum_{x \in \mathcal{X}_m} \mathbf{e}_m \left(hax^{-1} \right) \right| \left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right|.$$

Therefore,

$$\sum_{a=1}^{m} \left| M_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X}_m \frac{Y}{m} \right|^2 \leqslant \frac{1}{m^2} \sum_{a=1}^{m} E_{a,m}(\mathcal{X}, Y)^2. \tag{4}$$

We now put $J = \lfloor \log(Y/2) \rfloor - 1$ and define the sets

$$\begin{aligned}
\mathcal{H}_0 &= \left\{ h \mid 1 \leqslant |h| \leqslant \frac{m}{Y} \right\}, \\
\mathcal{H}_j &= \left\{ h \mid e^j \frac{m}{Y} < |h| \leqslant e^{j+1} \frac{m}{Y} \right\}, \qquad j = 1, \ldots, J, \\
\mathcal{H}_{J+1} &= \left\{ h \mid e^{J+1} \frac{m}{Y} < |h| \leqslant m/2 \right\},
\end{aligned}$$

(we can certainly assume that $J \geqslant 1$ since otherwise the bound is trivial).

By the Cauchy inequality we have

$$E_{a,m}(\mathcal{X}, Y)^2 \leqslant (J + 2) \sum_{j=0}^{J+1} E_{a,m,j}(\mathcal{X}, Y)^2, \tag{5}$$

where

$$E_{a,m,j}(\mathcal{X}, Y) = \sum_{h \in \mathcal{H}_j} \left| \sum_{x \in \mathcal{X}_m} \mathbf{e}_m \left(hax^{-1} \right) \right| \left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right|.$$

Using the bound

$$\left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right| = \left| \sum_{y=1}^{Y} \mathbf{e}_m(hy) \right| \ll \min\{Y, m/|h|\}$$

which holds for any integer h with $0 < |h| \leqslant m/2$, see [19, Bound (8.6)], we conclude that

$$\sum_{y=1}^{Y} \mathbf{e}_m(-hy) \ll e^{-j}Y, \qquad j = 0, \ldots, J+1.$$

Thus

$$E_{a,m,j}(\mathcal{X}, Y) \ll e^{-j}Y \left| \sum_{h \in \mathcal{H}_j} \vartheta_h \sum_{x \in \mathcal{X}_m} \mathbf{e}_m\left(hax^{-1}\right) \right|, \qquad j = 0, \ldots, J+1,$$

for some complex numbers ϑ_h with $|\vartheta_h| \leqslant 1$ for $|h| \leqslant m$. Therefore,

$$\begin{aligned}
\sum_{a=1}^{m} E_{a,m,j}(\mathcal{X}, Y)^2 &\ll e^{-2j}Y^2 \sum_{a=1}^{m} \left| \sum_{h \in \mathcal{H}_j} \vartheta_h \sum_{x \in \mathcal{X}_m} \mathbf{e}_m\left(hax^{-1}\right) \right|^2 \\
&= e^{-2j}Y^2 \sum_{a=1}^{m} \sum_{h_1, h_2 \in \mathcal{H}_j} \vartheta_{h_1}\vartheta_{h_2} \sum_{x_1, x_2 \in \mathcal{X}_m} \mathbf{e}_m\left(a\left(h_1x_1^{-1} - h_2x_2^{-1}\right)\right) \\
&= e^{-2j}Y^2 \sum_{h_1, h_2 \in \mathcal{H}_j} \vartheta_{h_1}\vartheta_{h_2} \sum_{x_1, x_2 \in \mathcal{X}_m} \sum_{a=1}^{m} \mathbf{e}_m\left(a\left(h_1x_1^{-1} - h_2x_2^{-1}\right)\right).
\end{aligned}$$

Clearly the inner sum vanishes if $h_1x_1^{-1} \not\equiv h_2x_2^{-1} \pmod m$ and is equal to m otherwise. Therefore

$$\sum_{a=1}^{m} E_{a,m,j}(\mathcal{X}, Y)^2 \ll e^{-2j}Y^2 mT_j, \tag{6}$$

where T_j is the number of solutions to the congruence

$$h_1x_2 \equiv h_2x_1 \pmod m, \qquad h_1, h_2 \in \mathcal{H}_j,\ x_1, x_2 \in \mathcal{X}_m.$$

We now see that if h_1 and x_2 are fixed then h_2 and x_1 are such that their product $s = h_2x_1 \ll e^j mX/Y$ belongs to a prescribed residue class modulo m. Thus there are at most $O\left(e^jX/Y + 1\right)$ possible values of s and for each fixed $s \ll e^j mX/Y$ there are $m^{o(1)}$ values of h_2 and x_1 with $s = h_2x_1$, see [29, Section I.5.2]. Therefore

$$T_j \leqslant \#\mathcal{X}\#\mathcal{H}_j \left(e^jX/Y + 1\right) m^{o(1)} = \frac{e^{2j}X\#\mathcal{X}m^{1+o(1)}}{Y^2} + \frac{e^j\#\mathcal{X}m^{1+o(1)}}{Y}$$

and after substitution into (6) we get

$$\sum_{a=1}^{m} E_{a,m,j}(\mathcal{X},Y)^2 \ll e^{-2j}Y^2 mT_j = X\#\mathcal{X}m^{2+o(1)} + e^{-j}\#\mathcal{X}Ym^{2+o(1)}.$$

A combination of this bound with (5) yields the inequality

$$\sum_{a=1}^{m} E_{a,m}(\mathcal{X},Y)^2 \leqslant J^2 X\#\mathcal{X}m^{o(1)} + \#\mathcal{X}Ym^{2+o(1)} = \#\mathcal{X}(X+Y)m^{2+o(1)}.$$

Finally, recalling (4), we conclude the proof. $\square$

Corollary 2. *For all positive integers m, X, Y, an arbitrary integer Z and the set $\mathcal{X} = \{x \in \mathbb{Z} \ : \ |x| \leqslant X\}$ we have*

$$\sum_{a=1}^{m} \left| M_{a,m}(\mathcal{X};Y,Z) - 2XY\frac{\varphi(m)}{m^2} \right|^2 \leqslant X(X+Y)m^{o(1)}.$$

Proof. Using the Möbius inversion formula involving the Möbius function $\mu(d)$, see [19, Section 1.3] or [29, Section I.2.5], we obtain

$$\sum_{\substack{|x|\leqslant X\\ \gcd(x,m)=1}} 1 = \sum_{d\mid m} \mu(d) \left(\frac{2X}{d} + O(1) \right) = 2X \sum_{d\mid m} \frac{\mu(d)}{d} + O\left(\sum_{d\mid m} |\mu(d)| \right).$$

Using that

$$\sum_{d\mid m} \frac{\mu(d)}{d} = \frac{\varphi(m)}{m}$$

see [29, Section I.2.7], and estimating

$$\sum_{d\mid m} |\mu(d)| \leqslant \sum_{d\mid m} 1 = m^{o(1)}$$

see [29, Section I.5.2], we derive

$$\sum_{\substack{|x|\leqslant X\\ \gcd(x,m)=1}} 1 = 2X\frac{\varphi(m)}{m} + O(m^{o(1)}). \tag{7}$$

which after substitution in Theorem 1 concludes the proof. $\square$

We now immediately derive from Corollary 2:

Corollary 3. *For all positive integers m, X, Y, an arbitrary integer Z, the set $\mathcal{X} = \{x \in \mathbb{Z} \ : \ |x| \leqslant X\}$ and an arbitrary real $\Gamma < 1$,*

$$\left| M_{a,m}(\mathcal{X}; Y, Z) - 2XY\frac{\varphi(m)}{m^2} \right| \geqslant \Gamma \frac{\varphi(m)}{m^2} XY$$

for at most $\Gamma^{-2} Y^{-1} \left(X^{-1} + Y^{-1} \right) m^{2+o(1)}$ values of $a = 1, \ldots, m$.

2.2 Multiples

We now estimate the average deviation between $N_{a,m}(\mathcal{X}; Y, Z)$ and its expected value taken over $a = 1, \ldots, m$. Our arguments are almost identical to those of Theorem 1, so we only indicate a few places where they differ (mostly only typographically). As before, if $\mathcal{X} \subseteq [-X, X]$ is dense enough, for example, if $\#\mathcal{X} \geqslant X m^{o(1)}$, this bound is nontrivial for $X, Y \geqslant m^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large m.

Theorem 4. *For all positive integers m, X, Y, an arbitrary integer Z and a set $\mathcal{X} \subseteq \{x \in \mathbb{Z} \ : \ |x| \leqslant X\}$,*

$$\sum_{a=1}^{m} \left| N_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X} \frac{Y}{m} \right|^2 \leqslant \#\mathcal{X}(X + Y) m^{o(1)}.$$

Proof. As in the proof of Theorem 1, we write

$$N_{a,m}(\mathcal{X}; Y, Z) = \sum_{x \in \mathcal{X}} \sum_{y=Z+1}^{Z+Y} \frac{1}{m} \sum_{-(m-1)/2 \leqslant h \leqslant m/2} \mathbf{e}_m \left(h(ax - y) \right)$$

and obtain, instead of (4), that

$$\sum_{a=1}^{m} \left| N_{a,m}(\mathcal{X}; Y, Z) - \#\mathcal{X} \frac{Y}{m} \right|^2 \leqslant \frac{1}{m^2} \sum_{a=1}^{m} F_{a,m}(\mathcal{X}, Y)^2 + Y^2 m^{-1+o(1)}$$

where

$$F_{a,m}(\mathcal{X}, Y) = \sum_{1 < |h| \leqslant m/2} \left| \sum_{x \in \mathcal{X}} \mathbf{e}_m \left(hax \right) \right| \left| \sum_{y=1}^{Y} \mathbf{e}_m(-hy) \right|.$$

Furthermore, instead of (5) we obtain

$$F_{a,m}(\mathcal{X},Y)^2 \leqslant (J+2)\sum_{j=0}^{J+1} F_{a,m,j}(\mathcal{X},Y)^2,$$

where

$$F_{a,m,j}(\mathcal{X},Y) = \sum_{h\in\mathcal{H}_j}\left|\sum_{x\in\mathcal{X}} \mathbf{e}_m\left(hax\right)\right|\left|\sum_{y=1}^{Y} \mathbf{e}_m(-hy)\right|,$$

with the same sets $\mathcal{H}_j$ as in the proof of Theorem 1. Accordingly, instead of (6) we get

$$\sum_{a=1}^{m} F_{a,m,j}(\mathcal{X},Y)^2 \ll e^{-2j}Y^2 m V_j,$$

where V_j is the number of solutions to the congruence

$$h_1x_1 \equiv h_2x_2 \pmod m, \qquad h_1,h_2\in\mathcal{H}_j,\ x_1,x_2\in\mathcal{X},\ \gcd(x_1x_2,m)=1.$$

Fixing h_1 and x_1 and counting the number of possibilities for the pair (h_2,x_2), as before, we obtain

$$V_j \leqslant \frac{e^{2j}X\#\mathcal{X}m^{1+o(1)}}{Y^2} + \frac{e^{j}\#\mathcal{X}m^{1+o(1)}}{Y},$$

which yields the desired result. □

Using (7), we deduce an analogue of Corollary 2.

Corollary 5. *For all positive integers m, X, Y, an arbitrary integer Z and the set $\mathcal{X}=\{x\in\mathbb{Z} \ :\ |x|\leqslant X\}$,*

$$\sum_{a=1}^{m}\left|M_{a,m}(\mathcal{X};Y,Z) - 2XY\frac{\varphi(m)}{m^2}\right|^2 \leqslant X(X+Y)m^{o(1)}.$$

We now immediately derive from Corollary 5

Corollary 6. *For all positive integers m, X, Y, an arbitrary integer Z, the set $\mathcal{X}=\{x\in\mathbb{Z} \ :\ |x|\leqslant X\}$ and an arbitrary real $\Gamma<1$,*

$$\left|N_{a,m}(\mathcal{X};Y,Z) - \frac{2XY}{m}\right| \geqslant \Gamma\frac{XY}{m},$$

for at most $\Gamma^{-2}Y^{-1}\left(X^{-1}+Y^{-1}\right)m^{2+o(1)}$ values of $a=1,\ldots,m$.

3 Distribution of Kloosterman sums

3.1 Distribution for a fixed prime

Let $\mathcal{Q}_{\alpha,\beta}(R,S,p)$ be the set of integers r and s with $|r| \leqslant R$, $|s| \leqslant S$, $\gcd(rs,p)=1$ and such that $\alpha \leqslant \psi_{r,s}(p) \leqslant \beta$.

Theorem 7. *For all primes p and positive integers R and S,*

$$\max_{0\leqslant\alpha<\beta\leqslant\pi} |\#\mathcal{Q}_{\alpha,\beta}(R,S,p) - 4\mu_{ST}(\alpha,\beta)RS| \ll RSp^{-1/4} + R^{1/2}S^{1/2}p^{1/2+o(1)}.$$

Proof. Let $\mathcal{A}_p(\alpha,\beta)$ be the set of integers a with $1 \leqslant a \leqslant p-1$ and such that $\alpha \leqslant \psi_{1,a}(p) \leqslant \beta$. By the result of Niederreiter [26], we have:

$$\max_{0\leqslant\alpha<\beta<\pi} |\#\mathcal{A}_p(\alpha,\beta) - \mu_{ST}(\alpha,\beta)p| \ll p^{3/4}. \tag{8}$$

Assume that $R \leqslant S$. Then, using that

$$K_{r,s}(p) = K_{1,rs}(p),$$

and defining the set

$$\mathcal{R} = \{r \in \mathbb{Z} \ : \ |r| \leqslant R\}, \tag{9}$$

we write,

$$\#\mathcal{Q}_{\alpha,\beta}(R,S,p) = \sum_{a\in\mathcal{A}_p(\alpha,\beta)} M_{a,p}(\mathcal{R}; 2S+1, -S-1) + O\left(RS/p\right),$$

where the term $O(RS/p)$ accounts for r and s with $\gcd(rs,p) > 1$. Thus the Cauchy inequality and Theorem 1 yield

$$\begin{aligned}
&\#\mathcal{Q}_{\alpha,\beta}(R,S,p) - \#\mathcal{A}_p(\alpha,\beta)\frac{2R(2S+1)}{p}\\
&\qquad \ll \sum_{a\in\mathcal{A}_p(\alpha,\beta)} \left| M_{a,p}(\mathcal{R}; 2S+1, -S-1) - \frac{2R(2S+1)}{p}\right| + RS/p\\
&\qquad \ll \left(p\sum_{a=1}^{p} \left| M_{a,p}(\mathcal{R}; 2S+1, -S-1) - \frac{2R(2S+1)}{p}\right|^2\right)^{1/2} + RS/p\\
&\qquad \ll \sqrt{R(R+S)}p^{1/2+o(1)} + RS/p.
\end{aligned}$$

Using (8) we see that for $R \leqslant S$,

$$\#\mathcal{Q}_{\alpha,\beta}(R,S,p) = 4\mu_{ST}(\alpha,\beta)RS + O\left(RSp^{-1/4} + R^{1/2}S^{1/2}p^{1/2+o(1)}\right)$$

uniformly over α and β.

For that $R > S$, we write,

$$\#\mathcal{Q}_{\alpha,\beta}(R,S,p) = \sum_{a\in\mathcal{A}_p(\alpha,\beta)} M_{a^{-1},p}(\mathcal{S}, 2R+1, -R-1)$$

where $\mathcal{S} = \{s \in \mathbb{Z} \ : \ |s| \leqslant S\}$, and proceed as before. $\square$

3.2 Sato–Tate conjecture on average

We start with an asymptotic formula for $\Pi_{\alpha,\beta}(R,S,T)$

Theorem 8. *For all positive integers R, S and T,*

$$\max_{0\leqslant\alpha<\beta\leqslant\pi} |\Pi_{\alpha,\beta}(R,S,T) - \mu_{ST}(\alpha,\beta)\pi(T)| \ll T^{3/4} + R^{-1/2}S^{-1/2}T^{3/2+o(1)}$$

Proof. We have

$$\Pi_{\alpha,\beta}(R,S,T) = \frac{1}{4RS}\sum_{p\leqslant T}\#\mathcal{Q}_{\alpha,\beta}(R,S,p)$$

Applying Theorem 7, after simple calculations we obtain the result. $\square$

Theorem 9. *For all positive integers R, S and T,*

$$\max_{0\leqslant\alpha<\beta\leqslant\pi} \Delta_{\alpha,\beta}(R,S,T) \ll T^{7/4} + R^{-1/2}S^{-1/2}T^{3+o(1)}$$

Proof. For two distinct primes p_1 and p_2, let $\mathcal{A}_{p_1p_2}(\alpha,\beta)$ be the set of integers a with $1 \leqslant a \leqslant p_1p_2 - 1$ and such that

$$a \equiv a_1 \pmod{p_1} \qquad \text{and} \qquad a \equiv a_2 \pmod{p_2},$$

with some $a_1 \in \mathcal{A}_{p_1}(\alpha,\beta)$ and $a_2 \in \mathcal{A}_{p_2}(\alpha,\beta)$.

Then, with the set $\mathcal{R}$ given by (9), we have

$$\begin{aligned}&\sum_{0<|r|\leqslant R}\sum_{0<|s|\leqslant S}\pi_{r,s}(\alpha,\beta;T)^2\\ &\qquad = 2\sum_{p_1<p_2\leqslant T}\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)}\left(M_{a,p_1p_2}(\mathcal{R};2S+1,-S-1) + O\left(\frac{RS}{p_1}\right)\right)\\ &\qquad\qquad + O(RST),\end{aligned}$$

where the term $O(RS/p_1)$ accounts for r and s with $\gcd(rs, p_1p_2) > 1$ and the term $O(RST)$ accounts for $p_1 = p_2$. Therefore,

$$\sum_{0<|r|\leqslant R}\sum_{0<|s|\leqslant S}\pi_{r,s}(\alpha,\beta;T)^2$$
$$= 2\sum_{p_1<p_2\leqslant T}\ \sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R}; 2S+1, -S-1) + O\left(RST^{1+o(1)}\right).$$

As in the proof of Theorem 7, we derive

$$\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R}; 2S+1, -S-1)$$
$$= 4\#\mathcal{A}_{p_1p_2}(\alpha,\beta)\frac{RS}{p_1p_2} + O\left(\sqrt{RS}(p_1p_2)^{1/2+o(1)}\right).$$

Thus, using (8) we obtain

$$\sum_{a\in\mathcal{A}_{p_1p_2}(\alpha,\beta)} M_{a,p_1p_2}(\mathcal{R}; 2S+1, -S-1)$$
$$= 4\mu_{ST}(\alpha,\beta)^2 RS + O\left(RSp_1^{-1/4} + \sqrt{RS}(p_1p_2)^{1/2+o(1)}\right).$$

Hence,

$$\sum_{0<|r|\leqslant R}\sum_{0<|s|\leqslant S}\pi_{r,s}(\alpha,\beta;T)^2$$
$$= 8\mu_{ST}(\alpha,\beta)^2 RS\sum_{p_1<p_2\leqslant T} 1 + O\left(RST^{7/4} + \sqrt{RS}T^{3+o(1)}\right)$$
$$= 4\mu_{ST}(\alpha,\beta)^2 RS\pi(T)^2 + O\left(RST^{7/4} + \sqrt{RS}T^{3+o(1)}\right).$$

Combining the above bound with Theorem 8, we derive the desired result. □

Clearly Theorems 8 and 9 are nontrivial under the conditions (2) and (3), respectively.

We also remark that combining [11, Lemma 4.4] (taken with $r = 1$) together with the method of [26], one can prove an asymptotic formula for $\#\mathcal{Q}_{\alpha,\beta}(1, S, p)$ for $S \geqslant p^{3/4+\varepsilon}$ for any fixed $\varepsilon > 0$. In turn, this leads to an asymptotic formula for $\Pi_{\alpha,\beta}(1, S, T)$ in the same range $S \geqslant T^{3/4+\varepsilon}$. However it is not clear how to estimate $\Delta_{\alpha,\beta}(R, S, T)$ within this approach.

References

[1] A. Akbary, C. David and R. Juricevic, 'Average distributions and products of special values of L-series', *Acta Arith.*, **111** (2004), 239–268.

[2] A. Adolphson, 'On the distribution of angles of Kloosterman sums', *J. Reine Angew. Math.*, **395** (1989), 214–220.

[3] S. Baier, 'The Lang–Trotter conjecture on average', *Preprint*, 2006.

[4] W. D. Banks, R. Heath-Brown and I. E. Shparlinski, 'On the average value of divisor sums in arithmetic progressions', *Intern. Math. Research Notices*, **2005** (2005), 1–25.

[5] J. Battista, J. Bayless, D. Ivanov and K. James, 'Average Frobenius distributions for elliptic curves with nontrivial rational torsion', *Acta Arith.*, **119** (2005), 81–91.

[6] C.-L. Chai and W.-C. W. Li, 'Character sums, automorphic forms, equidistribution, and Ramanujan graphs. I: The Kloosterman sum conjecture over function fields', *Forum Math.*, **15** (2003), 679–699.

[7] C. David and F. Pappalardi, 'Average Frobenius distributions of elliptic curves', *Internat. Math. Res. Notices*, **1999**, 165–183.

[8] C. David and F. Pappalardi, 'Average Frobenius distribution for inerts in $\mathbb{Q}(i)$', *J. Ramanujan Math. Soc.*, **19** (2004), 181–201.

[9] K. Ford, M. R. Khan, I. E. Shparlinski and C. L. Yankov, 'On the maximal difference between an element and its inverse in residue rings', *Proc. Amer. Math. Soc.*, **133** (2005), 3463–3468.

[10] É. Fouvry and P. Michel, 'Sur le changement de signe des sommes de Kloosterman', *Ann. Math.*, (to appear).

[11] É. Fouvry, P. Michel, J. Rivat and A. Sárközy, 'On the pseudorandomness of the signs of Kloosterman sums', *J. Aust. Math. Soc.*, **77** (2004), 425–436.

[12] É. Fouvry and M. R. Murty, 'On the distribution of supersingular primes', *Canad. J. Math.*, **48** (1996), 81–104.

[13] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a prime', *Monatsh. Math.*, **148** (2006), 127–138.

[14] M. Z. Garaev, 'On the logarithmic factor in error term estimates in certain additive congruence problems', *Acta Arith.*, **124** (2006), 27–39.

[15] M. Z. Garaev and A. A. Karatsuba, 'On character sums and the exceptional set of a congruence problem', *J. Number Theory*, **114** (2005), 182–192.

[16] M. Z. Garaev and A. A. Karatsuba, 'The representation of residue classes by products of small integers', *Preprint*, 2006.

[17] M. Z. Garaev and K.-L. Kueh, 'Distribution of special sequences modulo a large prime', *Int. J. Math. Math. Sci.*, **50** (2003), 3189–3194.

[18] E.-U. Gekeler, 'Frobenius distributions of elliptic curves over finite prime fields', *Int. Math. Res. Not.*, **2003**, no. 37, 1999–2018.

[19] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.

[20] K. James, 'Average Frobenius distributions for elliptic curves with 3-torsion', *J. Number Theory*, **109** (2004), 278–298.

[21] K. James and G. Yu, 'Average Frobenius distribution of elliptic curves', *Acta Arith.*, **124** (2006), 79–100.

[22] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Princeton Univ. Press, Princeton, NJ, 1988.

[23] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc, Providence, RI, 1999.

[24] G. Laumon, 'Exponential sums and l-adic cohomology: A survey', *Israel J. Math.*, **120** (2000), 225–257.

[25] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[26] H. Niederreiter, 'The distribution of values of Kloosterman sums', *Arch. Math.*, **56** (1991), 270–277.

[27] I. A. Semaev, 'On the number of small solutions of a linear homogeneous congruence', *Mat. Zametki*, **50** (1991), no.4, 102–107, (in Russian).

[28] I. A. Semaev, 'An algorithm for evaluation of discrete logarithms in some nonprime finite fields', *Math. Comp.*, **67** (1998), 1679–1689.

[29] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.